Studying the Locator Polynomials of Minimum Weight Codewords of BCH Codes

Daniel Augot, Pascale Charpin, and Nicolas Sendrier

Abstract—Only primitive binary cyclic codes of length $n = 2^m - 1$ are considered. A BCH-code with designed distance δ is denoted $B(n, \delta)$. A BCH-code is always a *narrow-sense* BCH-code. A codeword is identified with its *locator polynomial*, whose coefficients are the symmetric functions of the locators. The definition of the code by its zeros-set involves some properties for the power sums of the locators. Moreover, the symmetric functions and the power sums of the locators are related to Newton's *identities*. First presented is an algebraic point of view in order to prove or disprove the existence of words of a given weight in a code. The main tool is symbolic computation software to explore Newton's identities. The principal result is the true minimum distance of some BCH-codes of length 255 and 511, which were not known. In a second part, the minimum weight codewords of the codes $B(n, 2^h - 1)$ are studied. It is proven that the set of the minimum weight codewords of the BCH-code $B(n, 2^{m-2} - 1)$ equals the set of the minimum weight codewords of the punctured Reed–Muller code of length n and order 2, for any m. Several corollaries of this result are given.

Index Terms—Cyclic code, BCH-code, Reed–Muller code, locator polynomial, Newton's identities.

I. INTRODUCTION

IN this paper, we treat primitive binary cyclic codes. We are going to introduce a method for finding the true minimum distance of these codes.

We will first recall the usual definitions in Section II, as introduced in [11]. We can have an algebraic description of the codewords in a cyclic code, by studying their locator polynomials. This investigation of the locator polynomial of a codeword is achieved via the Newton's identities.

In Section III, we will show how to use the Newton's identities. In fact, we explore the identities in a progressive manner, using symbolic computation software. We have two options: either trying to establish a contradiction, or trying to find an effective solution of the Newton's identities. This method enables us to complete the table of the minimum distance of the BCH codes of length 255, and to extend our knowledge of BCH codes of length 511. Some of the longer proofs are given in Appendixes A, B, and C.

In Section IV, we give a description of the set of the minimum weight codewords of the BCH codes of length

$2^m - 1$ and designed distance $2^{m-2} - 1$ (Theorem 6). We prove that the locator polynomials of such codewords are, in fact, linearized polynomials. We obtain this result by studying Newton's identities associated to the minimum weight codewords of the BCH-codes of designed distance $2^h - 1$, $h \in [2, m - 1]$. Certain properties yield a complete characterization when $h = m - 2$. When $h \neq m - 2$, our proof involves an algorithm for constructing cyclic codes whose minimum weight codewords have linearized locator polynomials.

II. PRESENTATION AND NOTATIONS

Throughout this section we recall the usual conventions and notation as used in [11].

A. The BCH Codes and Their Minimum Distance

Let $n = 2^m - 1$. We denote by GF (q) the Galois field of order q, where $q = 2^m$ and denote by α a primitive nth root of unity in GF (q). Any cyclic code C of length n can be defined by its *generator polynomial* whose roots are called the zeros of the code C. Thus, we say that the defining set of C is the set

$$I(C) = \{i \in [0 \cdots n - 1] \mid \alpha^i \text{ is a zero of } C\}. \quad (1)$$

We denote by $cl(s)$ the cyclotomic class of s modulo n:

$$cl(s) = \{s, 2s, 2^2 s, \cdots, 2^{m-1} s \bmod n\}. \quad (2)$$

If α^i is a zero of C then α^{2i} is also a zero of C, so $I(C)$ is a union of cyclotomic classes $cl(s)$.

Thus, we can define the primitive narrow-sense BCH code of length n of designed distance δ, denoted by $B(n, \delta)$, as the cyclic code of length n whose defining set is the union of the cyclotomic classes $cl(1)$, $cl(2), \cdots, cl(\delta - 1)$. This "designed distance" terminology is used because of the well-known BCH-bound theorem.

Theorem 1: If the defining set of the cyclic code C contains a set of $\delta - 1$ consecutive integers (0 is treated consecutive to $n - 1$), then the minimum distance of C is at least δ.

So the code $B(n, \delta)$ has minimum distance at least δ. We are not satisfied by such a result. Generally the designed distance is equal to the minimum distance, but we have no systematic way of finding the true minimum distance. Of course there exist many other bounds for cyclic codes (J. H. van Lint and R. M. Wilson give an in-depth treatment of the subject in [13]), but these are not necessarily tight

bounds. It is a difficult problem to find the true minimum distance of long BCH codes.

The problem one encounters when looking for the true minimum distance is to work with the structure of the finite field GF (q) itself. This structure deeply influences the properties of cyclic codes, and bounds obtained from the properties of the defining set of a cyclic code do not reflect this underlying algebraic structure of GF (q).

B. Mattson–Solomon Polynomial and Locator Polynomial

Definition 1: The Mattson–Solomon polynomial of the word $x = (x_0, x_1, \cdots, x_{n-1})$ is the polynomial $A \in$ GF $(q)[Z]$:

$$A(z) = \sum_{i=1}^{i=n} A_i z^{n-i}, \tag{3}$$

where

$$A_i = x(\alpha^i) = \sum_{j=0}^{j=n-1} x_j \alpha^{ij}. \tag{4}$$

Remark:

- $A_{2i \bmod n} = A_i^2$
- $A_{i+n} = A_i$

So there is only one significant A_i for every cyclotomic class.

Definition 2: The locator polynomial $\sigma(Z)$ of a word x is

$$\sigma(Z) = \prod_{i=1}^{i=w} (1 - X_i Z), \tag{5}$$

where the X_i are the elements of GF (q) which are not zeros of the Mattson–Solomon polynomial of x. They are called the locators of x.

Definition 3: The elementary symmetric functions of the locators $X_1, X_2, \cdots, X_w$ are the σ_i:

$$\sigma_i = (-1)^i \sum_{1 \le k_1 < k_2 \cdots < k_i \le w} X_{k_1} X_{k_2} \cdots X_{k_i}$$

$$\text{if } 0 < i \le w$$

$$\sigma_0 = 1.$$

We have

$$\sigma(Z) = \sum_{i=0}^{i=w} \sigma_i Z^i. \tag{6}$$

The inversion formula of (3) (cf. [11] p. 240) implies that $A(\alpha^j) = x_j$. Hence, the zeros of the locator polynomial are the inverses of the locations of the nonzero coordinates of x.

In the case of binary codes, locators become very interesting, since binary words can be identified by their locators, and so by their locator polynomial.

We have the following property.

Proposition 1: Let x be a word of length n of weight w, with locators $X_1, X_2, \cdots, X_w$. Then x is in the cyclic code with defining set $\{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_l}\}$, if and only if the following power sum symmetric functions of its locators are zero:

$$A_{i_1} = A_{i_2} = \cdots = A_{i_l} = 0. \tag{7}$$

Recall that the kth power sum symmetric function of $X_1, \cdots, X_w$ is

$$A_k = \sum_{i=1}^{i=w} X_i^k \tag{8}$$

and is the kth coefficient of the Mattson–Solomon polynomial of x.

The following relations known as *Newton's identities* allow us to study the elementary symmetric functions, knowing the power sum symmetric functions.

Proposition 2: Let $X_1, X_2, \cdots, X_w$ be indeterminates over a field K, σ_i the elementary symmetric functions of the X_i and A_i the power sum symmetric functions of the X_i. Then, we have the following relations:

$$r \le w, \quad I_r: A_r + \sum_{i=1}^{i=r-1} A_{r-i}\sigma_i + r\sigma_r = 0,$$

$$r > w, \quad I_r: A_r + \sum_{i=1}^{i=w} A_{r-i}\sigma_i = 0. \tag{9}$$

C. The Locator Polynomial and BCH Codes

From the Newton's identities, we have the following result ([11, ch. 9, Lemma 4 p. 260]).

Lemma 1: Let

$$\sigma(Z) = \sum_{i=0}^{i=w} \sigma_i Z^i \tag{10}$$

be a polynomial over GF (2^m). Then $\sigma(Z)$ is the locator polynomial of a codeword x of $B(n, \delta)$, if and only if

a) $\sigma(Z)$ divides $Z^n - 1$.

b) $i \in [1, \delta - 1]$, i odd $\Rightarrow \sigma_i = 0$.

So we can try to find the true minimum distance of a code $B(n, \delta)$ by finding locator polynomials which satisfy conditions a) and b) of Lemma 1.

D. The Codes B(n, $2^k - 1$) and Linearized Polynomials

Definition 4: Let $l(Z)$ be a polynomial over GF (2^m). Then l(Z) is a linearized polynomial, if and only if

$$l(Z) = \sum_{i=0}^{i=l} a_i Z^{2^i}. \tag{11}$$

The interesting point about linearized polynomial is the following proposition ([11, ch. 4 p. 119]).

Proposition 3: $l(Z) \in$ GF $(2^m)[Z]$ is a linearized polynomial if and only if its zeros (eventually in an extension of GF (2^m)) form a vector space over GF (2).

Now we can prove as follows that the codes $B(n, \delta)$, $\delta = 2^k - 1$ have minimum distance δ.

a) Let H be a k-dimensional subspace of GF (2^m) over GF (2).

b) Then the polynomial: $l(Z) = \Pi_{z \in H}(Z - z)$ is a linearized polynomial.

c) It is easy to check that the polynomial $\sigma(Z) = \Pi_{y \in H}$ $_{y \ne 0}(1 - yZ)$ satisfies conditions a) and b) of Lemma 1.

Definition 5: The punctured Reed–Muller code of length n and order k, denoted by $\mathcal{R}(k, m)^*$ (cf. [11, p. 383]), is

the cyclic code of length $2^m - 1$ with the following defining set:

$$I(\mathcal{R}(k, m)^*) = \{i \in [1 \cdots n - 1] \mid w_2(i) < m - k\},$$

(12)

where $w_2(i)$ is the weight of the binary representation of i.

It is well known that the locators of any minimum weight codeword of the punctured Reed–Muller code of length $2^m - 1$ and order $m - k$, together with zero, form a k-dimensional GF (2)-subspace. So their locator polynomials have the following form:

$$\sigma(Z) = \sum_{i=0}^{i=k} \sigma_{2^k - 2^i} Z^{2^k - 2^i}.$$

(13)

In Section IV, we will use such a characterization of the minimum weight codewords of codes $\mathcal{R}(k, m)^*$.

III. The Minimum Distance of Some BCH Codes

Let C be any cyclic code of length n. GF(2^m) is the smallest field containing the nth roots of unity.

We consider Newton's identities (cf. (9)) written in term of w locators $X_1, X_2, \cdots, X_w$. Note that for a cyclic code C, A_i is replaced by 0, for all i in the defining set of C.

We call this set of equations, *Newton's identities for the code C and for the weight w.*

We call a set of A_i's and σ_i's that verify these identities, such that the polynomial $\sigma(z) = \sum_{i=0}^w \sigma_i z^i$ is square-free and splits in GF (2^m), a *solution* of this system.

Thus, the existence of solutions to Newton's identities for a code C and a weight w is equivalent to the existence of codewords of weight w in C.

We, therefore, have two ways of exploring the identities:

- either we prove the absence of a solution, so that there is no codeword of this weight in the code,
- or we find a solution, and this solution gives us a codeword of the given weight.

We use symbolic computation software to carry out this exploration, enabling us to manipulate the equations in their most general form (some of these have hundreds of terms). The method we use in both cases can roughly be described as follows.

1) We write down Newton's identities for a given code and a given weight.
2) We introduce into the equations the simplifications for the particular code in question.
3) We examine the equations one after another, trying either to express an indeterminate in terms of others, or to find a simple equation involving a small number of indeterminates.

Up to now we have not been able to make this exploration in a fully automatic manner; a user interface is necessary to make a proper choice at the critical stages of the search. There are many possible decisions at Step 3), including the decision to discard too large an equation, and it is difficult to make this choice efficiently within a program.

However, whenever possible we have implemented succes-sive refinements to our program, which now does most of these choices automatically.

We will use the following properties of the A_i's.

- $A_i^2 = A_{2i}$ and $A_{i+n} = A_i$, so there is exactly one relevant A_i for each cyclotomic class.
- $A_i^{2^{m'}} = A_i$ where m' is the cardinal of the cyclotomic class of i (this is a consequence of the previous property).
- If a codeword is shifted, each A_i is multiplied by α^i where α is the nth root of unity chosen for the defini-tion of the code. So, since $A_w \neq 0$, if n and w are relatively prime one can suppose that $A_w = 1$.

A. The Minimum Distance is Known for All Narrow-Sense Primitive Binary BCH Codes of Length 255

Theorem 2: All the narrow-sense primitive binary BCH codes of length 255 have their minimum distance equal to their designed distance except

- $B(255, 61)$, which has minimum distance 63,
- $B(255, 59)$, which has minimum distance 61.

Proof: From [4]–[6], [11], we know that all narrow-sense primitive BCH codes of length 255 reach the BCH bound except $B(255, 61)$ and $B(255, 59)$.

For both of these codes we are able to produce words of weight $\delta + 2$. Indeed

- $B(255, 61) \supset B(255, 63)$, and the latter code has mini-mum weight 63,
- for $B(255, 59)$, Dornstetter gives in [5] a word of weight 61.

Since the minimum distance of primitive BCH codes is odd, all we have to prove is that there are no codewords of weight 61 (resp. 59) in the code $B(255, 61)$ (resp. $B(255, 59)$). These results were obtained from a MAPLE program; traces of the computations are given in Appendixes A and B. □

B. The Minimum Distance is Known for Most Narrow-Sense Primitive Binary BCH Codes of Length 511

We found another code whose minimum distance exceeds the BCH bound.

Theorem 3: The code $B(511, 123)$ has minimum distance $d = 127$.

Proof:

a) $B(511, 123)$ is included in the punctured Reed–Muller code $\mathcal{R}(4, 9)^*$ (cf. Definition 5), and so has no code-word of weight 125, since $125 \equiv 1 \bmod 4$ [11, Corol-lary 13, p. 447];
b) $B(511, 127) \subset B(511, 123)$, and $B(511, 127)$ reaches the BCH bound.

From a) and b), we deduce easily that the minimum distance of $B(511, 123)$ is 123 or 127.

We show in Appendix C that there is no word of weight 123.   □

For codes of length 511 we also carried out another kind of search from Newton's identities: finding particular solutions by restricting the field of search. We introduced the following simplifications in the equations: all the A_i's and σ_i's are equal to 0 or 1. From the following lemma, this is exactly the same as looking for the idempotents of given weight.

Definition 6: The support of a word $x \in GF(q)^n$ is the set of its nonzero positions. We denote it by $\text{supp}(x)$.

Note that the support of a word of a cyclic code is the set of exponents of its locators.

Lemma 2: Let C be a binary cyclic code of length n, and let $GF(2^m)$ be the smallest field containing an nth root of unity. Let x be a word of C. The following assertions are equivalent:

a) x is an idempotent,
b) the support of x is the union of cyclotomic classes (in $GF(2^m)$),
c) the coefficients of the locator polynomial of x (the σ_i's) are in $GF(2)$,
d) the power sum symmetric functions of x (the A_i's) are in $GF(2)$.

Proof:

a) $\Rightarrow$ b) we have $x = x^2$. For any i,
$$i \in \text{supp}(x) \Rightarrow 2i \in \text{supp}(x^2) = \text{supp}(x).$$
So if $i \in \text{supp}(x)$ then $cl(i) \subset \text{supp}(x)$.
b) $\Rightarrow$ c) The roots of the locator polynomial $\sigma(z)$ are the inverses of the locators, so the set of the exponents of the roots is the union of cyclotomic classes and therefore, $\sigma(z) \in GF(2)[z]$.
c) $\Rightarrow$ d) If the σ_i's are given and are in $GF(2)$, then by induction, using Newton's identities, all the A_i's are in $GF(2)$.
d) $\Rightarrow$ a) Let A be the Mattson–Solomon polynomial of x. We have [11, Theorem 22, p. 240]:
$$x^2 = x \text{ (as polynomial)} \quad \Rightarrow A * A$$
$$= A \text{ (component wise product)}.$$

Since $A_j^2 = A_j$ for all j, we have $A * A = A$, and thus, $x^2 = x$.   □

This lemma is useful in two ways: it gives a way to find the idempotents from Newton's identities and a way to describe very simply an idempotent by giving its support as a union of cyclotomic classes.

We are able to find idempotents of given weight in some codes. For this search we give values in $GF(2)$ for some of the nonzero A_i's (8 of them for instance), and then the set of equations usually becomes easy to solve. It is possible to implement this exploration in a fully automatic manner.

Theorem 4: The code $B(511, \delta)$ contains idempotents of weight δ or $\delta + 1$ for
$$\delta = 19, 39, 45, 53, 57, 79, 83, 91, 103.$$

Proof: We look for codewords with power sum symmetric functions in $GF(2)$. From Lemma 2, these words are idempotents, and they are fully described by the cyclotomic classes partitioning their supports.

We give here, for a designed distance δ, the support of a codeword x of weight δ or $\delta + 1$:

$$\delta = 19, \quad \omega(x) = 19,$$
$$\text{supp}(x) = cl(0) \cup cl(23) \cup cl(91),$$
$$\delta = 39, \quad \omega(x) = 39,$$
$$\text{supp}(x) = cl(63) \cup cl(87) \cup cl(117)$$
$$\cup cl(127) \cup cl(219),$$
$$\delta = 45, \quad \omega(x) = 45,$$
$$\text{supp}(x) = cl(17) \cup cl(37) \cup cl(57) \cup cl(93) \cup cl(103),$$
$$\delta = 53, \quad \omega(x) = 54,$$
$$\text{supp}(x) = cl(17) \cup cl(31) \cup cl(41) \cup cl(45)$$
$$\cup cl(103) \cup cl(117),$$
$$\delta = 57, \quad \omega(x) = 57,$$
$$\text{supp}(x) = cl(29) \cup cl(43) \cup cl(51) \cup cl(55)$$
$$\cup cl(61) \cup cl(63) \cup cl(219),$$
$$\delta = 79, \quad \omega(x) = 79,$$
$$\text{supp}(x) = cl(0) \cup cl(3) \cup cl(13) \cup cl(39)$$
$$\cup cl(41) \cup cl(61) \cup cl(73)$$
$$\cup cl(77) \cup cl(107) \cup cl(117) \cup cl(219),$$
$$\delta = 83, \quad \omega(x) = 84,$$
$$\text{supp}(x) = cl(11) \cup cl(15) \cup cl(23) \cup cl(43)$$
$$\cup cl(53) \cup cl(79) \cup cl(123)$$
$$\cup cl(183) \cup cl(191) \cup cl(219),$$
$$\delta = 91, \quad \omega(x) = 91,$$
$$\text{supp}(x) = cl(0) \cup cl(7) \cup cl(13) \cup cl(25)$$
$$\cup cl(37) \cup cl(41) \cup cl(59) \cup cl(61)$$
$$\cup cl(117) \cup cl(175) \cup cl(239),$$
$$\delta = 103, \quad \omega(x) = 103,$$
$$\text{supp}(x) = cl(0) \cup cl(7) \cup cl(13) \cup cl(19)$$
$$\cup cl(27) \cup cl(31) \cup cl(87)$$
$$\cup cl(91) \cup cl(95) \cup cl(191)$$
$$\cup cl(219) \cup cl(223) \cup cl(255).$$

Since the true minimum distance d is odd, showing that a word has weight $\delta + 1$ is sufficient to prove that $d = \delta$.   □

Remarks:

- The weight of an idempotent cannot be an arbitrary integer, this integer has to be a sum of the cardinalities of some cyclotomic classes. For instance in $GF(512)$ we have one class with one element, 2 classes with 3, and

57 with 9. So the weight of an idempotent is a multiple of 9 plus 0, 1, 3, 4, 6 or 7 (each class can be used once). For instance, 29 cannot be the weight of an idempotent.

- We did not find an idempotent for every possible weight, but this is not surprising; the surprise is that we did find some. Since the set of idempotents and the set of minimum weight words are (very) small, their intersection should be empty most of the time.

Some other minimum distance are known for length 511. Table I gives a list of them as well as the way they were found. We try to give as reference the first author known to us who explicitly gives the code and its true minimum distance.

IV. THE MINIMUM WEIGHT CODEWORDS OF THE BCH-CODES $B(2^m - 1, 2^h - 1)$

We denote by $B(h)$, $h \in [2, m - 1]$, the BCH-code of length $2^m - 1$ and designed distance $2^h - 1$. Since $B(h)$ contains the minimum weight codewords (mwc's) of the punctured RM-code $\mathscr{R}(m - h, m)^*$, its minimum distance is exactly $2^h - 1$ (see Section II). However, the complete set of the mwc's of $B(h)$ is not known, except for the trivial cases:

$$B(2) = \mathscr{R}(m - 2, m)^*, \qquad B(m - 1) = \mathscr{R}(1, m)^*$$

and

$$B(3) = \mathscr{R}(2, 5)^*$$

(By identifying the defining sets). Thus, we suppose in general that

$$h \in [3, m - 2] \quad \text{and} \quad m > 5.$$

In this section, we want to give some answers to the following question: Is there a mwc of $B(h)$ which is not in $\mathscr{R}(m - h, m)^*$? On the other hand, it is natural to conjecture that for each h, there exists a cyclic code $C \neq \mathscr{R}(m - h, m)^*$, which is included in $B(h)$ and has for mwc's the mwc's of $\mathscr{R}(m - h, m)^*$.

Let C be a binary cyclic code of length $n = 2^m - 1$. We denote by $Mw(C)$ the set of the mwc's of C. We say that C has the property (RM$_h$), $h \in [3, m - 2]$, if and only if:

$$(\text{RM}_h): \quad \mathscr{R}(m - h, m)^* \subset C \subseteq B(h) \quad \text{and}$$

$$Mw(C) = Mw(\mathscr{R}(m - h, m)^*),$$

where the first inclusion is strict.

We shall prove (cf. Theorem 6) that the codes $B(m - 2)$ have the property (RM$_{m-2}$). We obtain this result by exploring Newton's identities of an mwc of a code $B(h)$, $h \in [3, m - 2]$; we study this general case and derive the result for $h = m - 2$. Moreover we can then provide an algorithm constructing cyclic codes which have the property (RM$_h$) for a given h.

Let x be a mwc of $B(h)$. We have seen that $x \in \mathscr{R}(m - h, m)^*$, if and only if its locator polynomial has the form $\sigma(Z) = \sum_{j=0}^{h} \sigma_{2^h-2^j} Z^{2^h - 2^j}$ (cf. (13)). Thus, we have the following reinterpretation of the property (RH$_h$).

TABLE I
BCH CODES OF LENGTH 511

n	k	δ	d	in	n	k	δ	d		in
511	502	3	3	[7]	511	241	73	73		[12]
	493	5	5	[7]		238	75	≥ 75		—
	484	7	7	[7]		229	77	≥ 77		—
	475	9	9	**		220	79	79		*
	466	11	11	[7]		211	83	83		*
	457	13	13	[6]		202	85	≥ 85		—
	448	15	15	[7]		193	87	≥ 87		—
	439	17	17	**		184	91	91		*
	430	19	19	*		175	93	95	#	[10]
	421	21	21	[12]		166	95	95		[7]
	412	23	23	[7]		157	103	103		*
	403	25	25	[6]		148	107	≥ 107		—
	394	27	27	[7]		139	109	111	#	[10]
	385	29	≥ 29	—		130	111	111		[7]
	376	31	31	[7]		121	117	119	#	[10]
	367	35	35	[12]		112	119	119		[7]
	358	37	≥ 37	—		103	123	127	##	*
	349	39	39	*		94	125	127	#	[10]
	340	41	≥ 41	—		85	127	127		[7]
	331	43	≥ 43	—		76	171	171		**
	322	45	45	*		67	175	175		**
	313	47	47	[7]		58	183	183		**
	304	51	≥ 51	—		49	187	187		**
	295	53	53	*		40	191	191		[7]
	286	55	55	[7]		31	219	219		[12]
	277	57	57	*		28	223	223		[7]
	268	59	≥ 59	—		19	239	239		[7]
	259	61	≥ 61	—		10	255	255		[7]
	250	63	63	[7]						

\# $d = \delta + 2$.
\# \# $d = \delta + 4$.
* New result obtained by Newton's identities.
** New result obtained by an exhaustive search.

Theorem 5: For each $h \in [2, m - 1]$, define:

$$J_h = \left\{ 2^h - 2^j \,\middle|\, j \in [0, h] \right\}. \tag{14}$$

Let x be a codeword of weight $2^h - 1$ and let $\sigma(Z) = \sum_{i=0}^{2^h-1} \sigma_i Z^i$ be the locator polynomial of x. Then x is a codeword of $\mathscr{R}(m - h, m)^*$, if and only if $\sigma_i = 0$ for all $i \notin J_h$.

Note that $0 \in J_h$ and that $j \in J_h - \{0\}$ implies $j \geq 2^{h-1}$; recall the following property of J_h due to Kasami *et al.*

Lemma 3 [9]: Let $h \in [2, m - 1]$, $i_0 = 2^h - 1$ and $r \in [1, i_0[$. Then,

a) $r \notin J_h \Rightarrow \omega_2(r + i_0) < h$.
b) $r \in J_h \Rightarrow \omega_2(r + i_0) = h$.

Let $S = [1, n]$, $n = 2^m - 1$. From now on we assume that any mwc x of $B(h)$ is defined by its locators $X_1, \cdots, X_{i_0}$. The corresponding power sum symmetric functions A_k, $k \in S$, and the elementary symmetric functions σ_r, $r \in [0, i_0]$ are related by the Newton's identities I_k, $k \in S$. By definition $\sigma_0 = 1$; since $x \in B(h)$ we know that

- $A_k = 0$, for $k \in [1, i_0[$,
- r odd and $r < i_0 \Rightarrow \sigma_r = 0$,
- A_{i_0} cannot be zero, since the minimum distance of $B(h)$ is exactly i_0.

Then identities I_k are satisfied for $k < i_0$; identity I_{i_0} yields $\sigma_{i_0} = A_{i_0}$. In accordance with Theorem 5, we shall study the

following hypothesis H_r:

H_r: $r \in [1, i_0[$ and $r \notin J_h \Rightarrow \sigma_r = 0$ and $A_{i_0+r} = 0$.

We know that H_r is true for r odd (cf. Lemma 1). Recall the form of identity I_{i_0+r}:

$$I_{i_0+r}: A_{i_0+r} + \sum_{k=1}^{r} A_{i_0+r-k}\sigma_k = 0. \tag{15}$$

The following lemma means that the code $B(h)$ has the property (RM_h), if and only if H_r is true for all $r \in [2, i_0[$, $i_0 = 2^h - 1$. This result still holds for any cyclic code C which contains $\mathscr{R}(m - h, m)^*$ and is contained in $B(h)$. We now proceed by induction on r to show that H_r is true.

Lemma 4: Let r be even. Suppose that $H_{r'}$ is true for all $r' \in [1, r[$. Then we have

$$I_{i_0+r}: A_{i_0+r} + A_{i_0}\sigma_r = 0.$$

Proof: We examine the term $A_{i_0+r-k}\sigma_k$ in (15), for $k \in [1, r[$:

- if $k \notin J_h$ then H_k implies $\sigma_k = 0$;
- if $k \in J_h$ then $k \geq 2^{h-1}$; hence $r - k < 2^{h-1}$, which means that $r - k$ is not in J_h; applying H_{r-k}, we obtain $A_{i_0+r-k} = 0$. $\quad\square$

Remark: We know that the locator polynomials of the mwc's of $\mathscr{R}(m - h, m)^*$ satisfy $\sigma_i = 0$ for $i \notin J_h$. From Lemma 4, we obtain another property:

$$r \in J_h \Rightarrow \sigma_r = \frac{A_{i_0+r}}{A_{i_0}}. \tag{16}$$

Example 1: The BCH-codes of designed distance 7, i.e., $h = 3$, $i_0 = 7$, and $J_3 = \{0, 4, 6, 7\}$. Recall that the defining-sets of $\mathscr{R}(m - 3, m)^*$ and $B(3)$ are

$$S_3 = \{s \in S \mid \omega_2(s) < 3\} \quad \text{and}$$
$$I(B(3)) = cl(1) \cup cl(3) \cup cl(5),$$

respectively. Since $\sigma_r = 0$ for r odd, Lemma 1 implies that $B(3)$ has the property (RM_3) if and only if $\sigma_2 = 0$; we have seen that H_1 is always true; from Lemma 4, $\sigma_2 = 0$ if and only if $A_9 = 0$. In other words: $B(3)$ has the property (RM_3) if and only if each mwc of $B(3)$ is such that $A_9 = 0$. We conjecture that, in general, $B(3)$ does not have the property (RM_3). For $m \in \{6, 7, 8, 9\}$, we have obtained (with a computer) a mwc of $B(3)$ which is not in $\mathscr{R}(m - 3, m)^*$.

Let $\hat{T} = cl(9) \cup I(B(3))$. Since $\omega_2(9) = 2$, $\hat{T} \subset S_3$. Now, we examine a code C whose defining-set T is such that $\hat{T} \subseteq T \subset S_3$, where the right inclusion is strict. Thus C contains $\mathscr{R}(m - 3, m)^*$ and is contained in $B(3)$. Moreover each codeword of C is such that its power sum symmetric function A_9 equals zero. If $m \in \{6, 7\}$, it is easy to see that $\hat{T}$ equals S_3. When $m > 7$, 17 is in S_3 and not in $\hat{T}$. In conclusion, we have the following.

1) Assume that $m > 7$. Then a cyclic code C with defining-set T satisfying:

$$cl(1) \cup cl(3) \cup cl(5) \cup cl(9) \subseteq T \subset \{s \in S \mid \omega_2(s) < 3\},$$

has the property (RM_3). Conversely, we conjecture that a code C which has the property (RM_3), satisfies the above property.

2) If $m \leq 7$, it is impossible to construct a code C which has the property (RM_3).

Now we will distinguish the two cases: $r \leq 2^{h-1}$ and $r > 2^{h-1}$.

Lemma 5: Assume that $r \in [2, 2^{h-1}]$, r even, and that $H_{r'}$ is true for all $r' < r$. Then identity I_{2i_0+3r} becomes

$$I_{2i_0+3r}: A_{2i_0+3r} + A_{i_0+r}^2\sigma_r + A_{i_0+3r}\sigma_{i_0} = 0,$$
$$\text{if } r > \frac{i_0 - 1}{3} \tag{17}$$

and

$$I_{2i_0+3r}: A_{2i_0+3r} + A_{i_0+r}^2\sigma_r + A_{i_0}^2\sigma_{3r} + A_{i_0+3r}\sigma_{i_0} = 0,$$
$$\text{if } r \leq \frac{i_0 - 1}{3}. \tag{18}$$

Proof: $i_0 = 2^h - 1$. Note that $2i_0 + 3r < 2^{h+1} + 3 \cdot 2^{h-1} < 2^m - 1$, since $h < m - 1$. Then the identity I_{2i_0+3r} is defined. Its general form is

$$I_{2i_0+3r}: A_{2i_0+3r} + \sum_{k=1}^{i_0-1} A_{2i_0+3r-k}\sigma_k + A_{i_0+3r}\sigma_{i_0} = 0. \tag{19}$$

Suppose that $H_{r'}$ is true for $r' < r$ and consider the term $A_{2i_0+3r-k}\sigma_k$. If k is odd, then $\sigma_k = 0$. If k is even, let $r - k = 2k'$; we have

$$A_{2(i_0+r)+r-k}\sigma_k = A_{i_0+r+k'}^2\sigma_k, \quad k \in [1, i_0[.$$

Then,

- $k' > 0 \Rightarrow k < r \Rightarrow \sigma_k = 0$, from H_k (k cannot be in J_h, since $r \leq 2^{h-1}$).
- $k' < 0$ and $r + k' \neq 0 \Rightarrow r + k' < r \Rightarrow A_{i_0+r+k'} = 0$ (if $r + k' > 0$ apply $H_{r+k'}$ otherwise $i_0 + r + k'$ is an element of the defining set of $B(h)$).
- $r + k' = 0$ is obtained when it is possible to have $k = 3r$; since $k < i_0$, this condition implies $r \leq (i_0 - 1)/3$.

In conclusion, identity I_{2i_0+3r} reduces to (17) if $r > (i_0 - 1)/3$ and to (18) otherwise. $\quad\square$

Lemma 6: r even and $i_0 = 2^h - 1$, $h \in [3, m - 2]$. Assume that $r \in [2^{h-1}, i_0[$ and $r \notin J_h$; suppose that $H_{r'}$ is true for all $r' < r$. Then identity $I_{2(i_0+r)}$ becomes

$$I_{2(i_0+r)}: A_{i_0+r}^2 + A_{i_0+2r}\sigma_{i_0} = 0. \tag{20}$$

Proof: Note that $2i_0 + 2r \leq 4i_0 - 2 \leq 2^{h+2} - 6 < 2^m - 1$. Hence, an identity I_{2i_0+2r} is defined. Its general form is

$$I_{2(i_0+r)}: A_{i_0+r}^2 + \sum_{k=1}^{i_0-1} A_{2(i_0+r)-k}\sigma_k + A_{i_0+2r}\sigma_{i_0} = 0. \tag{21}$$

Suppose that $H_{r'}$ is true for $r' < r$; consider for k even, the general term $A_{i_0+r-k'}^2\sigma_k$, where $k = 2k'$. Notice that, by

hypothesis,

$$k' < \frac{i_0}{2} \Rightarrow r - k' > 2^{h-1} - \frac{2^h - 1}{2} \Rightarrow 0 < r - k' < r.$$

Hence, if $r - k' \notin J_h$ then $A_{i_0 + r - k'} = 0$ (from $H_{r-k'}$). Suppose that $r - k' \in J_h$; then there is an integer $j \in [1, h - 1]$ such that $r - k' = 2^h - 2^j$. Now we have two possibilities.

1) $2k' < r$. If $k \notin J_h$ then $\sigma_k = 0$; if $k \in J_h$ there is a $j' \in [1, h - 1]$ such that $k = 2^h - 2^{j'}$; thus, $r = 2^h + 2^{h-1} - 2^j - 2^{j'-1}$; if $j < h - 1$ we obtain $r > 2^h - 1$; if $j = h - 1$ we obtain $r \in J_h$; so in all cases we have a contradiction to the hypothesis on r.
2) $2k' \geq r \Rightarrow r - k' \leq k' \leq (2^h - 2)/2$. Then $r - k'$ cannot be in J_h; that contradicts the hypothesis on $r - k'$.

Lemma 7: Assume that $h = m - 2$. Recall that the defining-set of $B(m - 2)$ is denoted by $I(B(m - 2))$ and that $i_0 = 2^h - 1$. The following properties are satisfied.

a) Let $s \in [0, 2^m - 1]$ and let $\sum_{k=0}^{m-1} s_k 2^k$ be the 2-ary expansion of s. Then $s \in I(B(h))$, if and only if there is $k < m$ and $j \notin \{k, k' = k + 1 (\mathrm{mod}\ m)\}$ such that $s_k = s_{k'} = s_j = 0$.
b) Let $r \in [2, 2^{h-1}[$, r even such that $i_0 + r \notin I(B(h))$. Then

$$2i_0 + 3r \in I(B(h)) \quad \text{and} \quad i_0 + 3r \in I(B(h)).$$

c) Let $r \in]2^{h-1}, i_0[$, r even and $r \notin J_h$. Then there is an element of the cyclotomic class of $i_0 + 2r$ (modulo $2^m - 1$), which can be written as

$$i_0 + \epsilon \quad \text{with } -i_0 < \epsilon < r \text{ and } \epsilon \notin J_h.$$

Proof: a) The hypotheses on s mean that $2^{m-k-1}s < 2^{m-2} - 1$, i.e., that s is an element of the defining-set of $B(m - 2)$.

b) Let $r' = r/2$. By hypothesis, the 2-ary expansion of i_0, r and r' are

$$i_0 = \sum_{j=0}^{m-3} 2^j, \qquad r = \sum_{j=1}^{m-4} r_j 2^j, \qquad r' = \sum_{j=0}^{m-5} r_{j+1} 2^j.$$

Note that $i_0 + r + r' < 2^{m-2} + 3.2^{m-4} - 1 < 2^{m-1}$. Let k be the smallest j such that $r_j \neq 0$. Suppose that $r_{k+1} = 0$ or that $k = m - 4$. We have

$$i_0 + r = \sum_{j=0}^{k-1} 2^j + (1 + 1)2^k + 2^{k+1}$$

$$+ \sum_{j=k+2}^{m-4} (1 + r_j)2^j + 2^{m-3}.$$

Then the 2-ary expansion of $i_0 + r$ is such that its kth term and its $(k + 1)$th term are zero. From a), that means $i_0 + r \in I(B(h))$, which contradicts the hypothesis. Thus $r_{k+1} = 1$

and $k < m - 4$. Now the 2-ary expansion of $i_0 + r + r'$ is

$$i_0 + r + r' = \sum_{j=0}^{k-2} 2^j + (1 + 0 + 1)2^{k-1} + (1 + 1 + 1)2^k$$

$$+ \sum_{j=k+1}^{m-5} (1 + r_j + r_{j+1})2^j$$

$$+ (1 + r_{m-4})2^{m-4} + 2^{m-3}$$

(by convention a sum from a to b, with $a > b$, equals 0). So we can see that the $(k - 1)$th term and the kth term are zero. We can apply a): the defining set of $B(h)$ contains $2(i_0 + r + r') = 2i_0 + 3r$. Now we have

$$i_0 + 3r < 2^{m-2} - 1 + 3.2^{m-3}$$

$$= 2^{m-1} + 2^{m-3} - 1 < 2^m - 1. \quad (22)$$

We consider the 2-ary expansion of $i_0 + 3r$:

$$i_0 + r + 2r = \sum_{j=0}^{k-1} 2^j + (1 + 1 + 0)2^k$$

$$+ (1 + 1 + 1)2^{k+1}$$

$$+ \sum_{j=k+2}^{m-4} (1 + r_j + r_{j-1})2^j$$

$$+ (1 + r_{m-4})2^{m-3}.$$

The kth term and the $(k + 1)$th term are zero. Moreover, from (22), an lth term, $l \in \{m - 1, m - 2, m - 3\}$ is zero. Applying a), we obtain $i_0 + 3r \in I(B(h))$.

c) By hypothesis, $2^{m-1} - 1 < i_0 + 2r < 2^m - 1$. We consider another element of the cyclotomic class of $i_0 + 2r$:

$$2(i_0 + 2r) - (2^m - 1) = i_0 + \epsilon,$$

where

$$\epsilon = 4r + 2^{m-2} - 2^m.$$

Since r is even and $2^{m-3} < r < 2^{m-2}$, we have

$$\epsilon > 4(2^{m-3} + 1) + 2^{m-2} - 2^m \Rightarrow \epsilon > 4 - 2^{m-2} > -i_0$$

and

$$\epsilon = r + 3(r - 2^{m-2}) \Rightarrow \epsilon < r - 3.$$

Suppose that $\epsilon \in J_h$. Then there is a $j \in [0, m - 2]$ such that

$$4r + 2^{m-2} - 2^m = 2^{m-2} - 2^j \Rightarrow r = 2^{m-2} - 2^{j-2},$$

which implies $r \in J_h$, contradicting the hypothesis. We have proved that ϵ cannot be in J_h.   □

Now we are able to prove that the code $B(m - 2)$ has the property (RM_{m-2}).

Theorem 6: The minimum weight codewords of the BCH-codes of length $2^m - 1$ and designed distance $2^{m-2} - 1$ are those of the punctured RM-code of the same length and order 2.

Proof: The notations are as previously defined; moreover assume that $h = m - 2$. We shall prove that, for this particular value of h, H_r is true for all $r \in [1, i_0[$. If r is

odd, we know that H_r is true; we suppose that $H_{r'}$ is true for all $r' \in [2, r[$ and we want to prove that H_r is true.

If $i_0 + r \in I(B(h))$ then $A_{i_0+r} = 0$ (by definition of $B(h)$); A_{i_0} cannot be zero, since the designed distance i_0 of $B(h)$ is exactly its minimum distance. Thus, Lemma 4 implies $\sigma_r = 0$; then H_r is true. So we suppose now that r is even and that $i_0 + r \notin I(B(h))$. We consider two cases.

1) Assume that $r \in [2, 2^{h-1}[$. Then r cannot be in J_h. Let ρ be the smallest element of $[i_0 + 1, 2 i_0[$, such that $\rho \notin I(B(m - 2))$. From Lemma 7a), we have

$$\rho = \begin{cases} \displaystyle\sum_{k=0}^{(m-2)/2} 2^{2k} = (2^m - 1)/3, & \text{if } m \text{ is even,} \\[2mm] 1 + \displaystyle\sum_{k=0}^{(m-3)/2} 2^{2k+1} \\[2mm] \quad = 1 + 2(2^{m-1} - 1)/3, & \text{if } m \text{ is odd.} \end{cases}$$

If we suppose that $i_0 + r \notin I(B(m - 2))$, then $i_0 + r \geq \rho$. If m is even then

$$\rho - i_0 = \frac{2^m - 1}{3} - 2^{m-2} + 1 = \frac{2^{m-2} + 2}{3},$$

and if m is odd then

$$\rho - i_0 = 1 + 2\frac{2^{m-1} - 1}{3} - 2^{m-2} + 1$$

$$= 1 + \frac{2^{m-2} + 1}{3}.$$

Hence, in all cases, $r > (i_0 - 1)/3$. From Lemma 5, the identity $I_{2i_0 + 3r}$ is reduced to (17). From Lemma 7b), $A_{2i_0+3r} = A_{i_0+3r} = 0$. Then

$$I_{2i_0+3r}: A_{i_0+r}^2 \sigma_r = 0 \quad \text{and} \quad I_{i_0+r}: A_{i_0+r} + A_{i_0}\sigma_r = 0,$$

which yields $A_{i_0+r} = 0$ and $\sigma_r = 0$, i.e., H_r is true.
2) Assume that $r \in [2^{h-1}, i_0[$. If $r \in J_h$ then H_r is true. So we suppose that $r \notin J_h$. From Lemma 7c), there is an ϵ, $-i_0 < \epsilon < r$ and $\epsilon \notin J_h$, such that $i_0 + \epsilon$ is an element of the cyclotomic class of $i_0 + 2r$; thus,

- $-i_0 < \epsilon < 0 \Rightarrow i_0 + \epsilon \in I(B(h)) \Rightarrow A_{i_0+\epsilon} = 0 \Rightarrow A_{i_0+2r} = 0$,
- $0 < \epsilon < r \Rightarrow A_{i_0+\epsilon} = 0$, (from H_ϵ) $\Rightarrow A_{i_0+2r} = 0$.

From Lemma 6, the identity $I_{2(i_0+r)}$ reduces to $A_{i_0+r}^2 = 0$. From Lemma 4, this yields $\sigma_r = 0$, i.e., H_r is true. In accordance with Theorem 5, we have proved that $B(m - 2)$ has the property (RM_{m-2}). Remark that $\mathscr{R}(2, m)^*$ is strictly contained in the code $B(m - 2)$; for instance $2^{m-1} - 2^{g+1} + 2^g - 1$, for $0 < g < m - 1$, is in the defining set of $\mathscr{R}(2, m)^*$ but not in $I(B(m - 2))$. $\qquad\square$

Let $x \in B(m - 2)$ such that $\omega(x) = 2^{m-2} = \mu$; let $X = \{X_1, \cdots, X_\mu\}$ be the set of locators of x. It is well known that the extended BCH-codes and the Reed–Muller codes are invariant under the affine group ([8], [2]); this means that, for each $g \in GF(2^m)$, the locators $\{X_1 + g, \cdots, X_\mu + g\}$

are those of a codeword in the extension of the code $B(m - 2)$. In particular, we can state

$$X = X_1 + \{0\} \cup X',$$

$$X' = \{X_2 + X_1, \cdots, X_\mu + X_1\},$$

where X' is the set of the locators of a codeword x' of $B(m - 2)$. Moreover x' is a mwc of $B(m - 2)$. Hence, Theorem 6 implies the following corollary.

Corollary 1: Let $x \in B(m - 2)$ be such that $\omega(x) = 2^{m-2}$. Then x is a codeword of the punctured RM-code $\mathscr{R}(2, m)^*$, i.e., the set of the locators of x is an $(m - 2)$-dimensional affine subspace of $GF(2^m)$.

It is well known that the automorphism group of the binary punctured Reed–Muller codes is the general linear group, denoted by $GL(2, m)$ ([11], p. 400); moreover the punctured RM-codes are generated by their mwc's ([11, p. 381]). Hence, a code C which has the property (RM_h) is such that its automorphism group is contained in $GL(2, m)$. Moreover, such a code cannot be generated by $Mw(C)$, since $\mathscr{R}(m - h, m)^*$ is strictly contained in it.

Corollary 2: $m > 5$. The automorphism group of the BCH-code $B(m - 2)$ is contained in $GL(2, m)$. The code generated by the set of the minimum weight codewords of $B(m - 2)$ is strictly contained in $B(m - 2)$.

The property (RM_3) is studied in Example 1, and Theorem 6 gives a general result for the property (RM_{m-2}). From now on, we are interested in the definition of cyclic codes which have the property (RM_h), for $h \in [4, m - 3]$, $m > 6$. We study the property (RM_h) by explaining the hypotheses on the mwc's of the codes $B(h)$. The main idea is that Newton's identities yield certain conditions on the power sum symmetric functions of these codewords. In accordance with Theorem 5 and Lemma 4, we can state a sufficient condition for a cyclic code to have the property (RM_h).

Corollary 3: Let us define

$$T_h = \bigcup_{s \in U_h} cl(s),$$

$$U_h = \{s \in [i_0 + 1, 2 i_0[\,| s \notin I(B(h)), \omega_2(s) < h\}. \quad (23)$$

Let C be a cyclic code such that its defining set T satisfies

$$I(B(h)) \cup T_h \subseteq T \subseteq \{s \in S | \omega_2(s) < h\}. \quad (24)$$

If $\mathscr{R}(m - h, m)^*$ is strictly contained in C, then C has the property (RM_h).

Proof: Suppose that $C \neq \mathscr{R}(m - h, m)^*$. Then the second inclusion in (24) is strict. From Lemma 3, the elements of T_h are of the form $s = i_0 + r$ with $r \notin J_h$. Then any mwc of C is a mwc of $B(h)$ which satisfies $A_{i_0+r} = 0$ for all $r \notin J_h$ (with $r \in [1, i_0[$). Applying Lemma 4, we prove by induction that H_r is true for all r. Then C has the property (RM_h). $\qquad\square$

The following conjectures are reinforced by results we

have obtained with a computer. For $h \in [4, m - 3]$, $m > 6$:

1) the codes $B(h)$ do not have the property (RM_h),
2) there exists a cyclic code C, the definition set of which is strictly contained in $I(B(h)) \cup T_h$, which has the property (RM_h).

We give later some examples which prove that the second conjecture is true for $m = 7$ and $m = 8$. We use the fact that the proof of Theorem 6, applied to the general case $h \neq m - 2$, provides an algorithm constructing a cyclic code which has the property (RM_h), for a given m. In the following, C is a cyclic code such that $\mathscr{R}(m - h, m)^* \subset C \subset B(h)$; T denotes its defining set. The proof of the proposed algorithm is obvious: using the results of Lemmas 4, 5, and 6, we construct T such that H_r is true for all $r \in [1, i_0)[$; if r is such that Newton's identities, given by (17) or (18) or (20), do not imply $A_{i_0+r} = 0$, then we add $i_0 + r$ in T.

Algorithm Constructing T

1) $T = I(B(h))$; $r = 0$; $i_0 = 2^h - 1$;
2) $r = r + 2$; IF $r > i_0$ THEN go to 8);
3) IF $i_0 + r \in T$ THEN put $\sigma_r := 0$ and GO TO 2);
4) IF $r < 2^{h-1}$, examine the identity I_{2i_0+3r}:
   IF I_{2i_0+3r}: $A_{i_0+r}^2 \sigma_r = 0$ THEN GO TO 7)
   ELSE PUT $T := T \cup cl(i_0 + r)$ and GO TO 7);
5) IF $r \in J_h$ THEN GO TO 2);
6) IF $r > 2^{h-1}$, examine the identity $I_{2(i_0+r)}$:
   IF $I_{2(i_0+r)}$: $A_{i_0+r}^2 = 0$ THEN GO TO 7)
   ELSE PUT $T := T \cup cl(i_0 + r)$;
7) PUT $\sigma_r := 0$ and $A_{i_0+r}^{2^j} := 0$, for $j \in [0, m - 1]$; GO TO 2);
8) END.

Example 2: $m = 7$; $h = 4$; thus $i_0 = 15$ and $J_4 = \{0, 8, 12, 14\}$. The code $B(h)$ is the BCH-code of length 127 and designed distance 15. In accordance with Corollary 3, we have $T_4 = cl(19) \cup cl(21)$. Using the algorithm, we obtain that the code C with defining set $T = I(B(4)) \cup cl(19)$, satisfies (RM_4).

Example 3: $m = 8$.

1) $h = 4$. The code $B(4)$ is the BCH-code of length 255 and designed distance 15. We have

$$T_4 = cl(17) \cup cl(19) \cup cl(21) \cup cl(25).$$

The algorithm produces: $T = I(B(4)) \cup cl(17) \cup cl(19)$.

2) $h = 5$; $J_5 = \{0, 16, 24, 28, 30, 31\}$. The code $B(5)$ is the BCH-code of length 255 and designed distance 31. We have

$$T_5 = cl(37) \cup cl(39) \cup cl(43) \cup cl(45)$$

$$\cup cl(51) \cup cl(53).$$

The algorithm produces: $T = I(B(5)) \cup cl(37) \cup cl(39)$.

APPENDIX A
$B(255, 61)$ HAS MINIMUM DISTANCE > 61

We consider Newton's identities I_r for $0 < r \le n = 255$, for the code $B(255, 61)$, and for the weight $\delta = 61$. We want to prove that there exists no codeword of weight δ.

The nonzero power sum symmetric functions of the code are

$$A_{61}, A_{63}, A_{85}, A_{87}, A_{91}, A_{95}, A_{111}, A_{119}, A_{127}.$$

Since 255 and 61 are relatively prime we can suppose $A_{61} = 1$ (the shift corresponds to a multiplication of each A_i by α^i).

In the case of a narrow-sense primitive BCH code, and for a weight equal to the designed distance, Newton's identities I_r (9) for odd r from $\delta + 2$ to $2\delta - 1$ form a triangular linear system giving the σ_i's for even i as polynomials depending on the nonzero A_i's. Here the system consists of the following 30 equations:

I_{63}: $A_{63} + \sigma_2 = 0$

I_{65}: $A_{63}\sigma_2 + \sigma_4 = 0$

I_{67}: $A_{63}\sigma_4 + \sigma_6 = 0$

I_{69}: $A_{63}\sigma_6 + \sigma_8 = 0$

I_{71}: $A_{63}\sigma_8 + \sigma_{10} = 0$

I_{73}: $A_{63}\sigma_{10} + \sigma_{12} = 0$

I_{75}: $A_{63}\sigma_{12} + \sigma_{14} = 0$

I_{77}: $A_{63}\sigma_{14} + \sigma_{16} = 0$

I_{79}: $1 + A_{63}\sigma_{16} + \sigma_{18} = 0$

I_{81}: $\sigma_2 + A_{63}\sigma_{18} + \sigma_{20} = 0$

I_{83}: $\sigma_4 + A_{63}\sigma_{20} + \sigma_{22} = 0$

I_{85}: $A_{85} + \sigma_6 + A_{63}\sigma_{22} + \sigma_{24} = 0$

I_{87}: $A_{87} + A_{85}\sigma_2 + \sigma_8 + A_{63}\sigma_{24} + \sigma_{26} = 0$

I_{89}: $A_{87}\sigma_2 + A_{85}\sigma_4 + \sigma_{10} + A_{63}\sigma_{26} + \sigma_{28} = 0$

I_{91}: $A_{91} + A_{87}\sigma_4 + A_{85}\sigma_6 + \sigma_{12} + A_{63}\sigma_{28} + \sigma_{30} = 0$

I_{93}: $A_{87}^4 + A_{91}\sigma_2 + A_{87}\sigma_6 + A_{85}\sigma_8 + \sigma_{14} + A_{63}\sigma_{30} + \sigma_{32} = 0$

I_{95}: $A_{95} + A_{87}^4\sigma_2 + A_{91}\sigma_4 + A_{87}\sigma_8 + A_{85}\sigma_{10} + \sigma_{16}$
$\qquad + A_{63}\sigma_{32} + \sigma_{34} = 0$

I_{97}: $A_{95}\sigma_2 + A_{87}^4\sigma_4 + A_{91}\sigma_6 + A_{87}\sigma_{10} + A_{85}\sigma_{12} + \sigma_{18}$
$\qquad + A_{63}\sigma_{34} + \sigma_{36} = 0$

I_{99}: $A_{95}\sigma_4 + A_{87}^4\sigma_6 + A_{91}\sigma_8 + A_{87}\sigma_{12} + A_{85}\sigma_{14} + \sigma_{20}$
$\qquad + A_{63}\sigma_{36} + \sigma_{38} = 0$

I_{101}: $A_{95}\sigma_6 + A_{87}^4\sigma_8 + A_{91}\sigma_{10} + A_{87}\sigma_{14} + A_{85}\sigma_{16} + \sigma_{22}$
$\qquad + A_{63}\sigma_{38} + \sigma_{40} = 0$

I_{103}: $A_{95}\sigma_8 + A_{87}^4\sigma_{10} + A_{91}\sigma_{12} + A_{87}\sigma_{16} + A_{85}\sigma_{18} + \sigma_{24}$
$\qquad + A_{63}\sigma_{40} + \sigma_{42} = 0$

I_{105}: $A_{95}\sigma_{10} + A_{87}^4\sigma_{12} + A_{91}\sigma_{14} + A_{87}\sigma_{18} + A_{85}\sigma_{20} + \sigma_{26}$
$\qquad + A_{63}\sigma_{42} + \sigma_{44} = 0$

I_{107}: $A_{91}^{32} + A_{95}\sigma_{12} + A_{87}^4\sigma_{14} + A_{91}\sigma_{16} + A_{87}\sigma_{20}$

$\qquad + A_{85}\sigma_{22} + \sigma_{28} + A_{63}\sigma_{44} + \sigma_{46} = 0$

I_{109}: $A_{91}^4 + A_{91}^{32}\sigma_2 + A_{95}\sigma_{14} + A_{87}^4\sigma_{16} + A_{91}\sigma_{18} + A_{87}\sigma_{22}$

$\qquad + A_{85}\sigma_{24} + \sigma_{30} + A_{63}\sigma_{46} + \sigma_{48} = 0$

I_{111}: $A_{111} + A_{91}^4\sigma_2 + A_{91}^{32}\sigma_4 + A_{95}\sigma_{16} + A_{87}^4\sigma_{18} + A_{91}\sigma_{20}$

$\qquad + A_{87}\sigma_{24} + A_{85}\sigma_{26} + \sigma_{32} + A_{63}\sigma_{48} + \sigma_{50} = 0$

I_{113}: $A_{111}\sigma_2 + A_{91}^4\sigma_4 + A_{91}^{32}\sigma_6 + A_{95}\sigma_{18} + A_{87}^4\sigma_{20} + A_{91}\sigma_{22}$

$\qquad + A_{87}\sigma_{26} + A_{85}\sigma_{28} + \sigma_{34} + A_{63}\sigma_{50} + \sigma_{52} = 0$

I_{115}: $A_{111}\sigma_4 + A_{91}^4\sigma_6 + A_{91}^{32}\sigma_8 + A_{95}\sigma_{20} + A_{87}^4\sigma_{22} + A_{91}\sigma_{24}$

$\qquad + A_{87}\sigma_{28} + A_{85}\sigma_{30} + \sigma_{36} + A_{63}\sigma_{52} + \sigma_{54} = 0$

I_{117}: $A_{87}^{16} + A_{111}\sigma_6 + A_{91}^4\sigma_8 + A_{91}^{32}\sigma_{10} + A_{95}\sigma_{22} + A_{87}^4\sigma_{24}$

$\qquad + A_{91}\sigma_{26} + A_{87}\sigma_{30} + A_{85}\sigma_{32}$
$\qquad + \sigma_{38} + A_{63}\sigma_{54} + \sigma_{56} = 0$

I_{119}: $A_{119} + A_{87}^{16}\sigma_2 + A_{111}\sigma_8 + A_{91}^4\sigma_{10} + A_{91}^{32}\sigma_{12} + A_{95}\sigma_{24}$

$\qquad + A_{87}^4\sigma_{26} + A_{91}\sigma_{28} + A_{87}\sigma_{32}$
$\qquad + A_{85}\sigma_{34} + \sigma_{40} + A_{63}\sigma_{56} + \sigma_{58} = 0$

I_{121}: $A_{119}\sigma_2 + A_{87}^{16}\sigma_4 + A_{111}\sigma_{10} + A_{91}^4\sigma_{12} + A_{91}^{32}\sigma_{14}$

$\qquad + A_{95}\sigma_{26} + A_{87}^4\sigma_{28} + A_{91}\sigma_{30} + A_{87}\sigma_{34}$
$\qquad + A_{85}\sigma_{36} + \sigma_{42} + A_{63}\sigma_{58} + \sigma_{60} = 0$,

which gives us the following values for the σ_i's:

$$\sigma_2 := A_{63}$$

$$\sigma_4 := A_{63}^2$$

$$\sigma_6 := A_{63}^3$$

$$\sigma_8 := A_{63}^4$$

$$\sigma_{10} := A_{63}^5$$

$$\sigma_{12} := A_{63}^6$$

$$\sigma_{14} := A_{63}^7$$

$$\sigma_{16} := A_{63}^8$$

$$\sigma_{18} := 1 + A_{63}^9$$

$$\sigma_{20} := A_{63}^{10}$$

$$\sigma_{22} := A_{63}^2 + A_{63}^{11}$$

$$\sigma_{24} := A_{85} + A_{63}^{12}$$

$$\sigma_{26} := A_{87} + A_{63}^4 + A_{63}^{13}$$

$$\sigma_{28} := A_{85}A_{63}^2 + A_{63}^{14}$$

$$\sigma_{30} := A_{91} + A_{87}A_{63}^2 + A_{63}^6 + A_{63}^{15}$$

$$\sigma_{32} := A_{87}^4 + A_{85}A_{63}^4 + A_{63}^{16}$$

$$\sigma_{34} := A_{95} + A_{91}A_{63}^2 + A_{87}A_{63}^4 + A_{63}^8 + A_{63}^{17}$$

$$\sigma_{36} := A_{87}^4A_{63}^2 + A_{85}A_{63}^6 + 1 + A_{63}^{18}$$

$$\sigma_{38} := A_{95}A_{63}^2 + A_{91}A_{63}^4 + A_{87}A_{63}^6 + A_{63}^{10} + A_{63} + A_{63}^{19}$$
$$\sigma_{40} := A_{87}^4A_{63}^4 + A_{85}A_{63}^8 + A_{63}^{20}$$

$$\sigma_{42} := A_{95}A_{63}^4 + A_{91}A_{63}^6 + A_{87}A_{63}^8 + A_{63}^{12} + A_{63}^{21}$$

$$\sigma_{44} := A_{87}^4A_{63}^6 + A_{85}A_{63}^{10} + A_{63}^4 + A_{63}^{22}$$

$$\sigma_{46} := A_{91}^{32} + A_{95}A_{63}^6 + A_{91}A_{63}^8 + A_{87}A_{63}^{10} + A_{63}^{14} + A_{63}^5 + A_{63}^{23}$$

$$\sigma_{48} := A_{91}^4 + A_{87}^4A_{63}^8 + A_{85}^2 + A_{85}A_{63}^{12} + A_{63}^{24}$$

$$\sigma_{50} := A_{111} + A_{91}^{32}A_{63}^2 + A_{95}A_{63}^8 + A_{91}A_{63}^{10}$$
$$\qquad + A_{87}A_{63}^{12} + A_{63}^{16} + A_{63}A_{85}^2 + A_{63}^{25}$$

$$\sigma_{52} := A_{63}^8 + A_{87}^2 + A_{63}^{26} + A_{91}^4A_{63}^2$$
$$\qquad + A_{87}^4A_{63}^{10} + A_{85}A_{63}^{14}$$

$$\sigma_{54} := 1 + A_{63}^9 + A_{91}^{32}A_{63}^4 + A_{63}^{27} + A_{95}A_{63}^{10} + A_{91}A_{63}^{12}$$
$$\qquad + A_{87}A_{63}^{14} + A_{63}A_{87}^2 + A_{111}A_{63}^2 + A_{63}^{18}$$

$$\sigma_{56} := A_{91}^4A_{63}^4 + A_{87}^{16} + A_{63}^{28} + A_{87}^4A_{63}^{12} + A_{85}^2A_{63}^4 + A_{85}A_{63}^{16}$$

$$\sigma_{58} := A_{111}A_{63}^4 + A_{119} + A_{63}^{29} + A_{91}^{32}A_{63}^6 + A_{95}A_{63}^{12}$$
$$\qquad + A_{91}A_{63}^{14} + A_{87}A_{63}^{16}A + A_{85}^2A_{63}^5 + A_{63}^{20}$$

$$\sigma_{60} := A_{85} + A_{91}^2 + A_{87}^2A_{63}^4 + A_{85}A_{63}^{18} + A_{87}^{16}A_{63}^2$$
$$\qquad + A_{91}^4A_{63}^6 + A_{87}^4A_{63}^{14} + A_{63}^{30} + A_{63}^{12}.$$

The other values are $\sigma_0 = 1$, by definition, and $\sigma_i = 0$ for odd i, given by the first δ identities.

After replacement of the σ_i's by their values, the remaining equations are sorted in terms of increasing size of the number of monomials:

186, 190, 188, 194, 198, 192, 202, 123, 184, 189, 191, 196, 206, 254, 127, 195, 200, 210, 135, 193, 187, 199, 214, 125, 131, 204, 252, 197, 222, 203, 238, 129, 139, 208, 250, 143, 201, 218, 133, 137, 226, 230, 246, 248, 234, 185, 212, 242, 207, 141, 181, 216, 236, 244, 151, 183, 205, 220, 232, 147, 224, 159, 179, 211, 240, 149, 175, 155, 145, 157, 209, 173, 163, 167, 228, 153, 171, 215, 253, 251, 165, 169, 161, 177, 213, 223, 239, 247, 249, 243, 217, 235, 237, 245, 219, 221, 229, 231, 233, 227, 225, 241.

We will proceed as follows.

- We successively check the equations in the order given above, up to a "solvable" one.
- After solving one equation, we restart from the beginning.
  (At each stage we substitute all the known A_i's in the current equation, and we simplify it as much as possible.)

We give here, in order of resolution, all the "solvable" equations, and the way we used them:

I_{186}: $A_{87}^8 + A_{85}^2A_{63}^8 + A_{85}A_{63}^{20} + A_{87}^{16}A_{63}^4 + A_{91}^4A_{63}^8$

$\qquad + A_{87}^4A_{63}^{16} + A_{63}^{32} + A_{95}^4 = 0$

$\qquad \Rightarrow A_{95} := A_{87}^2 + A_{85}^2A_{63}^2 + A_{85}A_{63}^5 + A_{87}^4A_{63}$

$\qquad\qquad + A_{91}A_{63}^2 + A_{87}A_{63}^4 + A_{63}^8$

$$I_{188}: A_{87}^8 A_{63} + A_{91}^2 A_{63}^3 + A_{87}^2 A_{63}^7 + A_{85}^2 + A_{85}^2 A_{63}^9$$

$$+ A_{91} + A_{87} A_{63}^2 + A_{63}^6 + A_{63}^{15} + A_{127} = 0$$

$$\Rightarrow A_{127} := A_{87}^8 A_{63} + A_{91}^2 A_{63}^3 + A_{87}^2 A_{63}^7 + A_{85}^2$$

$$+ A_{85}^2 A_{63}^9 + A_{91} + A_{87} A_{63}^2 + A_{63}^6 + A_{63}^{15}$$

$$I_{194}: A_{85}^3 + 1 = 0 \Rightarrow A_{85} \neq 0$$

$$I_{198}: A_{85} A_{87}^2 + A_{63}^2 = 0 \Rightarrow A_{87} := A_{63} A_{85}$$

$$I_{187}: 1 + A_{91} A_{85} A_{63}^{18} + A_{85}^2 A_{91} A_{63}^6 + A_{91}^4 A_{63}^{21} + A_{63}^2$$

$$+ A_{63}^{142} + A_{63}^{130} A_{85} + A_{111}^{128} A_{63}^2 + A_{91}^{16} A_{63}^3$$

$$+ A_{85}^2 A_{63}^{39} + A_{119}^8 + A_{91}^6 A_{63}^9 + A_{91}^2 A_{63}^{33} + A_{91}^4 A_{63}^3$$

$$+ A_{85}^2 A_{91}^2 + A_{85}^2 A_{63}^{21} + A_{63}^{36} + A_{63}^{15} A_{85} + A_{91} A_{63}^{30}$$

$$+ A_{91}^3 + A_{85} A_{63}^{24} + A_{85}^2 A_{63}^{15} A_{91}^4 + A_{91}^2 A_{63}^{21} A_{85}$$

$$+ A_{63}^9 A_{85} A_{91}^4 + A_{91}^4 A_{63}^{12} + A_{91}^2 A_{63}^6 + A_{91}^5 A_{63}^6$$

$$+ A_{85}^2 A_{91}^4 A_{63}^6 + A_{85}^2 A_{63}^{30} + A_{63}^{45}$$

$$+ A_{91} A_{85} + A_{91} A_{63}^{12} + A_{63}^3 A_{85}^2 = 0$$

$$\Rightarrow A_{119} := 1 + A_{111}^{16} A_{63}^{64} + A_{85} A_{63}^{228} + A_{91}^{160} A_{63}^{192}$$

$$+ A_{91}^{32} A_{85}^2 A_{63}^{66} + A_{63}^{64} + A_{85} A_{63}^{225} A_{91}^{128}$$

$$+ A_{63}^{80} A_{85}^2 + A_{63}^{225} A_{85}^2 + A_{91}^{32} A_{63}^{195} + A_{85} A_{63}^{195}$$

$$+ A_{91}^2 A_{63}^{96} + A_{91}^{64} A_{85} + A_{63}^{132} + A_{91}^{128} A_{63}^{96}$$

$$+ A_{91}^{192} A_{63}^{33} + A_{91}^{64} A_{63}^{162} A_{85}^2 + A_{63}^{96} A_{85}$$

$$+ A_{63}^{33} A_{85}^2 A_{91}^{128} + A_{85} A_{91}^{128} A_{63}^{192} + A_{91}^{32} A_{63}^{129}$$

$$+ A_{63}^{209} + A_{91}^{128} A_{63}^{162} + A_{63}^{165} + A_{85} A_{91}^{32} A_{63}^{192}$$

$$+ A_{63}^3 A_{85}^2 + A_{91}^{128} A_{63}^{129} + A_{91}^{64} A_{63}^{36} + A_{85} A_{63}^{162}$$

$$+ A_{91}^{64} A_{63}^{192} + A_{91}^{96} + A_{91}^{32} A_{85}^2$$

$$I_{189}: A_{91}^2 A_{63}^{34} + A_{91}^4 A_{85} A_{63}^{10} + A_{91} A_{63}^{31} + A_{63} A_{91}^3$$

$$+ A_{91}^4 A_{63}^4 + A_{85} A_{63}^{25} + A_{85}^2 A_{63}^{22} + A_{91} A_{85} A_{63}^{19}$$

$$+ A_{63}^7 A_{91}^2 + A_{91}^4 A_{63}^{13} + A_{91}^5 A_{63}^7 + A_{85}^2 A_{63}^{31} A_{63}$$

$$+ A_{63}^2 + A_{63}^{128} A_{91} + A_{63}^{37} + A_{111}^4 + A_{91} A_{63}^{13}$$

$$+ A_{91}^4 A_{63}^{22} + A_{63}^{128} A_{85}^2 + A_{91}^2 A_{63} A_{85}^2 + A_{85}^2 A_{63}^4$$

$$+ A_{85} A_{63}^{16} + A_{63}^3 + A_{63}^{134} + A_{85}^2 A_{63}^{40} + A_{91}^6 A_{63}^{10}$$

$$+ A_{63}^{46} + A_{85}^2 A_{91} A_{63}^7 + A_{85}^2 A_{63}^{16} A_{91}^4 + A_{91}^2 A_{63}^{22} A_{85}$$

$$+ A_{85}^2 A_{91}^4 A_{63}^7 + A_{63} A_{91} A_{85} = 0$$

$$\Rightarrow A_{111} := A_{91} A_{85}^2 A_{63}^4 + A_{63}^{133} A_{85}^2 + A_{91} A_{85} A_{63}^{130}$$

$$+ A_{91}^{64} A_{85} A_{63}^{196} + A_{91}^{128} A_{63}^{64} A_{85}^2 + A_{85}^2 A_{91}^{64} A_{63}^{193}$$

$$+ A_{63}^{70} A_{85} + A_{63}^{64} + A_{63}^{128} + A_{63}^{139} + A_{85}^2 A_{63}^{10}$$

$$+ A_{91}^{129} A_{63}^{130} + A_{91}^{128} A_{63}^{133} A_{85} + A_{85}^2 A_{91} A_{63}^{193}$$

$$+ A_{63} A_{85}^2 + A_{63}^{32} A_{85}^2 + A_{63}^{64} A_{91}^{64} A_{85} + A_{63}^{73}$$

$$+ A_{91} A_{63} + A_{85} A_{63}^4 + A_{63}^{133} A_{91} + A_{91}^{65} A_{63}^{193}$$

$$+ A_{85}^2 A_{63}^{199} + A_{91}^{64} A_{63}^{67} + A_{63}^{161} + A_{91}^{64} A_{63}^{199}$$

$$+ A_{91} A_{63}^{67} + A_{91}^{128} A_{63}^{136} + A_{63}^{193} A_{91}^{128} + A_{63}^{32} A_{91}^{64}$$

$$+ A_{63}^{192} + A_{63}^{64} A_{91}^{192}$$

$$I_{199}: A_{91}^{16} = 0 \Rightarrow A_{91} := 0$$

$$I_{203}: 1 = 0.$$

APPENDIX B
$B(255, 59)$ HAS MINIMUM DISTANCE > 59

We consider Newton's identities I_r for $0 < r \leq n = 255$, for the code $B(255, 59)$, and for the weight $\delta \doteq 59$. We want to prove that there exists no codeword of weight δ.

The nonzero power sum symmetric functions of the code are

$$A_{59}, A_{61}, A_{63}, A_{85}, A_{87}, A_{91}, A_{95}, A_{111}, A_{119}, A_{127}.$$

Since 255 and 59 are relatively prime we can suppose $A_{59} = 1$.

We will first solve the triangular linear system giving the σ_i's for even i as polynomials depending on the nonzero A_i's. The system consists of the following 29 equations:

$$I_{61}: A_{61} + \sigma_2 = 0$$

$$I_{63}: A_{63} + A_{61} \sigma_2 + \sigma_4 = 0$$

$$I_{65}: A_{63} \sigma_2 + A_{61} \sigma_4 + \sigma_6 = 0$$

$$I_{67}: A_{63} \sigma_4 + A_{61} \sigma_6 + \sigma_8 = 0$$

$$I_{69}: A_{63} \sigma_6 + A_{61} \sigma_8 + \sigma_{10} = 0$$

$$I_{71}: A_{63} \sigma_8 + A_{61} \sigma_{10} + \sigma_{12} = 0$$

$$I_{73}: A_{63} \sigma_{10} + A_{61} \sigma_{12} + \sigma_{14} = 0$$

$$I_{75}: A_{63} \sigma_{12} + A_{61} \sigma_{14} + \sigma_{16} = 0$$

$$I_{77}: A_{63} \sigma_{14} + A_{61} \sigma_{16} + \sigma_{18} = 0$$

$$I_{79}: A_{61}^{64} + A_{63} \sigma_{16} + A_{61} \sigma_{18} + \sigma_{20} = 0$$

$$I_{81}: A_{61}^{64} \sigma_2 + A_{63} \sigma_{18} + A_{61} \sigma_{20} + \sigma_{22} = 0$$

$$I_{83}: A_{61}^{64} \sigma_4 + A_{63} \sigma_{20} = A_{61} \sigma_{22} + \sigma_{24} = 0$$

$$I_{85}: A_{85} + A_{61}^{64} \sigma_6 + A_{63} \sigma_{22} + A_{61} \sigma_{24} + \sigma_{26} = 0$$

$$I_{87}: A_{87} + A_{85} \sigma_2 + A_{61}^{64} \sigma_8 + A_{63} \sigma_{24} + A_{61} \sigma_{26} + \sigma_{28} = 0$$

$$I_{89}: A_{87} \sigma_2 + A_{85} \sigma_4 + A_{61}^{64} \sigma_{10} + A_{63} \sigma_{26} + A_{61} \sigma_{28} + \sigma_{30} = 0$$

$$I_{91}: A_{91} + A_{87} \sigma_4 + A_{85} \sigma_6 + A_{61}^{64} \sigma_{12} + A_{63} \sigma_{28}$$
$$+ A_{61} \sigma_{30} + \sigma_{32} = 0$$

$$I_{93}: A_{87}^4 + A_{91} \sigma_2 + A_{87} \sigma_6 + A_{85} \sigma_8 + A_{61}^{64} \sigma_{14} + A_{63} \sigma_{30}$$
$$+ A_{61} \sigma_{32} + \sigma_{34} = 0$$

$$I_{95}: A_{95} + A_{87}^4 \sigma_2 + A_{91} \sigma_4 + A_{87} \sigma_8 + A_{85} \sigma_{10} + A_{61}^{64} \sigma_{16}$$
$$+ A_{63} \sigma_{32} + A_{61} \sigma_{34} + \sigma_{36} = 0$$

$$I_{97}: A_{95} \sigma_2 + A_{87}^4 \sigma_4 + A_{91} \sigma_6 + A_{87} \sigma_{10} + A_{85} \sigma_{12} + A_{61}^{64} \sigma_{18}$$
$$+ A_{63} \sigma_{34} + A_{61} \sigma_{36} + \sigma_{38} = 0$$

$$I_{99}: A_{95} \sigma_4 + A_{87}^4 \sigma_6 + A_{91} \sigma_8 + A_{87} \sigma_{12} + A_{85} \sigma_{14} + A_{61}^{64} \sigma_{20}$$
$$+ A_{63} \sigma_{36} + A_{61} \sigma_{38} + \sigma_{40} = 0$$

$$I_{101}: A_{95} \sigma_6 + A_{87}^4 \sigma_8 + A_{91} \sigma_{10} + A_{87} \sigma_{14} + A_{85} \sigma_{16} + A_{61}^{64} \sigma_{22}$$
$$+ A_{63} \sigma_{38} + A_{61} \sigma_{40} + \sigma_{42} = 0$$

$$I_{103}: 1 + A_{95} \sigma_8 + A_{87}^4 \sigma_{10} + A_{91} \sigma_{12} + A_{87} \sigma_{16} + A_{85} \sigma_{18}$$
$$+ A_{61}^{64} \sigma_{24} + A_{63} \sigma_{40} + A_{61} \sigma_{42} + \sigma_{44} = 0$$

$$I_{105}: \sigma_2 + A_{95}\sigma_{10} + A_{87}^4\sigma_{12} + A_{91}\sigma_{14} + A_{87}\sigma_{18} + A_{85}\sigma_{20}$$
$$+ A_{61}^{64}\sigma_{26} + A_{63}\sigma_{42} + A_{61}\sigma_{44} + \sigma_{46} = 0$$

$$I_{107}: A_{91}^{32} + \sigma_4 + A_{95}\sigma_{12} + A_{87}^4\sigma_{14} + A_{91}\sigma_{16} + A_{87}\sigma_{20}$$
$$+ A_{85}\sigma_{22} + A_{61}^{64}\sigma_{28} + A_{63}\sigma_{44} + A_{61}\sigma_{46} + \sigma_{48} = 0$$

$$I_{109}: A_{91}^4 + A_{91}^{32}\sigma_2 + \sigma_6 + A_{95}\sigma_{14} + A_{87}^4\sigma_{16} + A_{91}\sigma_{18}$$
$$+ A_{87}\sigma_{22} + A_{85}\sigma_{24} + A_{61}^{64}\sigma_{30} + A_{63}\sigma_{46}$$
$$+ A_{61}\sigma_{48} + \sigma_{50} = 0$$

$$I_{111}: A_{111} + A_{91}^4\sigma_2 + A_{91}^{32}\sigma_4 + \sigma_8 + A_{95}\sigma_{16} + A_{87}^4\sigma_{18}$$
$$+ A_{91}\sigma_{20} + A_{87}\sigma_{24} + A_{85}\sigma_{26} + A_{61}^{64}\sigma_{32}$$
$$+ A_{63}\sigma_{48} + A_{61}\sigma_{50} + \sigma_{52} = 0$$

$$I_{113}: A_{111}\sigma_2 + A_{91}^4\sigma_4 + A_{91}^{32}\sigma_6 + \sigma_{10} + A_{95}\sigma_{18} + A_{87}^4\sigma_{20}$$
$$+ A_{91}\sigma_{22} + A_{87}\sigma_{26} + A_{85}\sigma_{28}$$
$$+ A_{61}^{64}\sigma_{34} + A_{63}\sigma_{50} + A_{61}\sigma_{52} + \sigma_{54} = 0$$

$$I_{115}: A_{111}\sigma_4 + A_{91}^4\sigma_6 + A_{91}^{32}\sigma_8 + \sigma_{12} + A_{95}\sigma_{20} + A_{87}^4\sigma_{22}$$
$$+ A_{91}\sigma_{24} + A_{87}\sigma_{28} + A_{85}\sigma_{30}$$
$$+ A_{61}^{64}\sigma_{36} + A_{63}\sigma_{52} + A_{61}\sigma_{54} + \sigma_{56} = 0$$

$$I_{117}: A_{87}^{16} + A_{111}\sigma_6 + A_{91}^4\sigma_8 + A_{91}^{32}\sigma_{10} + \sigma_{14} + A_{95}\sigma_{22}$$
$$+ A_{87}^4\sigma_{24} + A_{91}\sigma_{26} + A_{87}\sigma_{30}$$
$$+ A_{85}\sigma_{32} + A_{61}^{64}\sigma_{38} + A_{63}\sigma_{54} + A_{61}\sigma_{56} + \sigma_{58} = 0$$

$$I_{119}: A_{119} + A_{87}^{16}\sigma_2 + A_{111}\sigma_8 + A_{91}^4\sigma_{10} + A_{91}^{32}\sigma_{12} + \sigma_{16}$$
$$+ A_{95}\sigma_{24} + A_{87}^4\sigma_{26} + A_{91}\sigma_{28}$$
$$+ A_{87}\sigma_{32} + A_{85}\sigma_{34} + A_{61}^{64}\sigma_{40} + A_{63}\sigma_{56} + A_{61}\sigma_{58} = 0,$$

which gives us the following values for the σ_i's:

$$\sigma_2 := A_{61}$$

$$\sigma_4 := A_{61}^2 + A_{63}$$

$$\sigma_6 := A_{61}^3$$

$$\sigma_8 := A_{63}A_{61}^2 + A_{63}^2 + A_{61}^4$$

$$\sigma_{10} := A_{61}A_{63}^2 + A_{61}^5$$

$$\sigma_{12} := A_{63}^3 + A_{63}A_{61}^4 + A_{61}^6$$

$$\sigma_{14} := A_{61}^7$$

$$\sigma_{16} := A_{63}^4 + A_{63}^2A_{61}^4 + A_{63}A_{61}^6 + A_{61}^8$$

$$\sigma_{18} := A_{61}A_{63}^4 + A_{63}^2A_{61}^5 + A_{61}^9$$

$$\sigma_{20} := A_{61}^{64} + A_{63}^5 + A_{63}^3A_{61}^4 + A_{63}A_{61}^8 + A_{61}^2A_{63}^4 + A_{61}^{10}$$

$$\sigma_{22} := A_{61}^3A_{63}^4 + A_{61}^{11}$$

$$\sigma_{24} := A_{61}^{66} + A_{63}^6 + A_{63}^2A_{61}^8 + A_{61}^2A_{63}^5 + A_{63}A_{61}^{10} + A_{61}^{12}$$

$$\sigma_{26} := A_{85} + A_{61}A_{63}^6 + A_{63}^2A_{61}^9 + A_{61}^{13}$$

$$\sigma_{28} := A_{87} + A_{61}^{64}A_{63}^2 + A_{61}^{68} + A_{63}^7 + A_{63}^3A_{61}^8 + A_{63}A_{61}^{12} + A_{61}^{14}$$

$$\sigma_{30} := A_{85}A_{61}^2 + A_{61}^{15}$$

$$\sigma_{32} := A_{91} + A_{87}A_{61}^2 + A_{61}^{70} + A_{63}^8 + A_{63}^4A_{61}^8 + A_{63}^2A_{61}^{12}$$
$$+ A_{63}A_{61}^{14} + A_{61}^{16}$$

$$\sigma_{34} := A_{87}^4 + A_{85}A_{63}^2 + A_{85}A_{61}^4 + A_{61}A_{63}^8 + A_{63}^4A_{61}^9$$
$$+ A_{63}^2A_{61}^{13} + A_{61}^{17}$$

$$\sigma_{36} := A_{95} + A_{61}^{18} + A_{61}^{72} + A_{63}^9 + A_{91}A_{61}^2 + A_{87}A_{63}^2 + A_{87}A_{61}^4$$
$$+ A_{61}^{64}A_{63}^4 + A_{61}^{68}A_{63}^2 + A_{63}^5A_{61}^8 + A_{63}^3A_{61}^{12} + A_{63}A_{61}^{16}$$
$$+ A_{61}^2A_{63}^8 + A_{63}^4A_{61}^{10}$$

$$\sigma_{38} := A_{85}A_{61}^6 + A_{61}^3A_{63}^8 + A_{63}^4A_{61}^{11} + A_{61}^{19} + A_{87}^4A_{61}^2$$

$$\sigma_{40} := A_{61}^{128} + A_{63}^6A_{61}^8 + A_{63}^2A_{61}^{16} + A_{61}^2A_{63}^9 + A_{63}^5A_{61}^{10}$$
$$+ A_{61}^4A_{63}^8 + A_{61}^{66}A_{63}^4 + A_{95}A_{61}^2 + A_{91}A_{63}^2 + A_{91}A_{61}^4$$
$$+ A_{61}^{74} + A_{63}^{10} + A_{61}^{20} + A_{87}A_{61}^6 + A_{63}A_{61}^{18}$$

$$\sigma_{42} := A_{85}A_{63}^2A_{61}^4 + A_{87}^4A_{63}^2 + A_{87}^4A_{61}^4 + A_{85}A_{63}^4 + A_{85}A_{61}^8$$
$$+ A_{63}^6A_{61}^9 + A_{63}^2A_{61}^{17} + A_{61}^5A_{63}^8 + A_{61}A_{63}^{10} + A_{61}^{129} + A_{61}^{21}$$

$$\sigma_{44} := 1 + A_{87}A_{63}^2A_{61}^4 + A_{63}A_{61}^{128} + A_{61}^{22} + A_{61}^{76} + A_{63}^{11}$$
$$+ A_{95}A_{63}^2 + A_{95}A_{61}^4 + A_{91}A_{61}^6 + A_{87}A_{63}^4 + A_{87}A_{61}^8$$
$$+ A_{61}^{64}A_{63}^6 + A_{61}^{72}A_{63}^2 + A_{63}^7A_{61}^8 + A_{63}^3A_{61}^{16} + A_{61}^4A_{63}^9$$
$$+ A_{63}A_{61}^{20} + A_{61}^6A_{63}^8$$

$$\sigma_{46} := A_{85}A_{61}^2A_{63}^4 + A_{61}^7A_{63}^8 + A_{61}^{23} + A_{87}^4A_{61}^6 + A_{85}A_{61}^{10}$$

$$\sigma_{48} := A_{91}A_{63}^2A_{61}^4 + A_{87}A_{61}^2A_{63}^4 + A_{63}^{12} + A_{61}^{24} + A_{61}^{132} + A_{61}^{78}$$
$$+ A_{61}^2 + A_{91}^{32} + A_{95}A_{61}^6 + A_{91}A_{63}^4 + A_{91}A_{61}^8 + A_{87}A_{61}^{10}$$
$$+ A_{63}^{22}A_{61}^2 + A_{63}^4A_{61}^{16} + A_{61}^4A_{63}^{10} + A_{63}^2A_{61}^{20} + A_{61}^6A_{63}^9$$

$$\sigma_{50} := A_{91}^4 + A_{85}A_{61}^{12} + A_{61}A_{63}^{12} + A_{63}^4A_{61}^{17} + A_{61}^5A_{63}^{10}$$
$$+ A_{63}^2A_{61}^{21} + A_{85}A_{63}^2A_{61}^8 + A_{87}^4A_{63}^2A_{61}^4 + A_{61}^{25} + A_{61}^{133}$$
$$+ A_{87}^4A_{63}^4 + A_{87}^4A_{61}^8 + A_{85}A_{63}^6$$

$$\sigma_{52} := A_{61}^4 + A_{63}^2 + A_{61}^{64}A_{63}^8 + A_{61}^{72}A_{63}^4 + A_{61}^{76}A_{63}^2 + A_{63}A_{61}^{24}$$
$$+ A_{63}A_{61}^{132} + A_{63}^5A_{61}^{16} + A_{61}^4A_{63}^{11} + A_{63}^3A_{61}^{20} + A_{61}^2A_{63}^{12}$$
$$+ A_{63}^4A_{61}^{18} + A_{61}^{80} + A_{63}^{13} + A_{61}^{26} + A_{95}A_{63}^2A_{61}^4$$
$$+ A_{91}A_{61}^2A_{63}^4 + A_{87}A_{63}^2A_{61}^8 + A_{95}A_{63}^4 + A_{87}A_{61}^{12}$$
$$+ A_{91}^{32}A_{61}^2 + A_{95}A_{61}^8 + A_{87}A_{63}^6 + A_{91}A_{61}^{10} + A_{85}^2 + A_{111}$$

$$\sigma_{54} := A_{87}^4A_{61}^2A_{63}^4 + A_{85}A_{61}^{14} + A_{61}A_{85}^2 + A_{61}^3A_{63}^{12} + A_{63}^4A_{61}^{19}$$
$$+ A_{61}^{27} + A_{87}^4A_{61}^{10} + A_{91}^4A_{61}^2$$

$$\sigma_{56} := A_{91}A_{63}^2A_{61}^8 + A_{95}A_{61}^2A_{63}^4 + A_{63}^{14} + A_{87}^2 + A_{61}^{82} + A_{61}^{136}$$
$$+ A_{61}^{28} + A_{111}A_{61}^2 + A_{91}^{32}A_{63}^2 + A_{91}^{32}A_{61}^4 + A_{95}A_{61}^{10}$$
$$+ A_{91}A_{63}^6 + A_{91}A_{61}^{12} + A_{87}A_{61}^{14} + A_{61}^{128}A_{63}^4 + A_{61}^{66}A_{63}^8$$
$$+ A_{61}^{74}A_{63}^4 + A_{63}A_{85}^2 + A_{63}^2A_{61}^{24} + A_{63}^6A_{61}^{16} + A_{61}^2A_{63}^{13}$$
$$+ A_{63}^5A_{61}^{18} + A_{63}A_{61}^{26} + A_{61}^6$$

$$\sigma_{58} := A_{85}A_{63}^2A_{61}^{12} + A_{85}A_{63}^4A_{61}^8 + A_{87}^4A_{63}^2A_{61}^8 + A_{87}^{16}$$
$$+ A_{61}^{129}A_{63}^4 + A_{61}A_{63}^{14} + A_{61}A_{87}^2 + A_{63}^2A_{61}^{25} + A_{63}^6A_{61}^{17}$$
$$+ A_{61}^{137} + A_{61}^{29} + A_{91}A_{63}^2 + A_{91}A_{61}^4 + A_{87}^4A_{63}^6 + A_{87}^4A_{61}^{12}$$
$$+ A_{85}A_{63}^8 + A_{85}A_{61}^{16}.$$

The other values are $\sigma_0 = 1$, by definition, and $\sigma_i = 0$ for odd i, given by the first identities.

After replacement of the σ_i's by their values, the remaining equations will be sorted in increasing size (number of monomials) order:

180, 188, 196, 192, 186, 184, 204, 200, 190, 252, 189, 119, 178, 182, 187, 212, 121, 194, 208, 220, 236, 198, 125, 185, 244, 191, 193, 202, 248, 197, 216, 228, 224, 123, 133, 195, 129, 206, 232, 250, 240, 205, 137, 141, 201, 181, 183, 246, 254, 218, 127, 199, 210, 173, 179, 203, 157, 253, 131, 214, 177, 149, 171, 234, 249, 139, 145, 153, 222, 242, 230, 135, 251, 169, 238, 245, 155, 165, 213, 221, 209, 207, 237, 241, 217, 226, 147, 175, 161, 143, 243, 163, 151, 211, 167, 247, 233, 235, 219, 159, 229, 225, 239, 227, 215, 231, 223.

We will proceed as follows.

- We successively check the equations in the order given above, up to a "solvable" one;
- After solving one equation, we restart from the beginning.
  (at each stage we substitute all the known A_i's, and we show the most simple equation possible.)

We will first show that $A_{61} \neq 0$.
Suppose that $A_{61} = 0$. Then

$$I_{196}: A_{85}^3 = 0 \Rightarrow A_{85} := 0,$$

$$I_{208}: A_{87}^6 = 0 \Rightarrow A_{87} := 0,$$

$$I_{236}: 1 = 0,$$

so $A_{61} \neq 0$.

We give here, in order of resolution, all the "solvable" equations, and the way we used them:

$$I_{180}: A_{61}^8 A_{85} A_{63}^4 + A_{85} A_{63}^8 + A_{61}^4 A_{91}^4 + A_{61}^{29}$$
$$+ A_{61}^3 A_{85}^2 + A_{61}^{16} A_{85} + A_{61}^{12} A_{87}^4 + A_{87}^{16} = 0$$

$$\Rightarrow A_{91} := A_{61} A_{85} A_{63} + A_{61}^{254} A_{85} A_{63}^2 + A_{61}^2 A_{87} + A_{61}^{70}$$
$$+ A_{61}^{191} A_{85}^2 + A_{61}^3 A_{85} + A_{61}^{254} A_{87}^4$$

$$I_{196}: A_{95}^2 A_{61}^3 + A_{87}^8 A_{61} A_{63}^2 + A_{85}^2 A_{61} A_{63}^6 + A_{87}^2 A_{61}^3 A_{63}^4$$
$$+ A_{85}^3 + A_{61}^{131} + A_{63}^8 + A_{61}^{139} A_{63}^4$$
$$+ A_{61}^{130} A_{87}^4 + A_{61}^5 A_{85}^2 A_{63}^4 = 0$$

$$\Rightarrow A_{95} := A_{61}^{126} A_{85}^3 + A_{61}^{254} A_{87}^4 A_{63} + A_{61}^{254} A_{85} A_{63}^3 + A_{87} A_{63}^2$$
$$+ A_{61} A_{85} A_{63}^2 + A_{61}^{64} A_{63}^4 + A_{61}^{68} A_{63}^2 + A_{61}^{191} A_{87}^2$$

$$I_{192}: A_{85}^3 = 0 \Rightarrow A_{85} = 0$$

$$I_{200}: 1 = 0. \qquad \square$$

APPENDIX C
$B(511, 123)$ HAS MINIMUM DISTANCE > 123

We consider Newton's identities for $0 < i \leq n = 511$ for the code $B(511, 123)$, and for the weight $\delta = 123$. We want to prove that there exists no codeword of weight δ.

The nonzero power sum symmetric functions of the code are

$$A_{123}, A_{125}, A_{127}, A_{171}, A_{175}, A_{183}, A_{187},$$
$$A_{191}, A_{219}, A_{223}, A_{239}, A_{255}.$$

Since 511 and 123 are relatively prime we can suppose $A_{123} = 1$.

We will give an abbreviated proof for this code (the complete proof is too long to present here).

We will first solve the linear triangular system giving the σ_i's for even i as polynomials depending on the nonzero A_i's. The σ_i's for odd i are null. We consider that the σ_i's have been substituted in the equations.

Furthermore we will suppose $A_{125} \neq 0$ (when $A_{125} = 0$, we found a contradiction).

We give here the equations we used for the resolution, and the way we used them:

$$I_{372}: A_{125}^{63} + A_{171}^8 A_{125}^{13} + A_{171}^{32} A_{125}^5 + A_{171}^4 A_{127}^8 A_{125}^{22}$$
$$+ A_{171}^4 A_{125}^6 A_{127}^{16} + A_{187}^4 A_{125}^6 + A_{175}^{16} A_{125}^2 + A_{183}^4 A_{125}^{14}$$
$$+ A_{171}^4 A_{125}^{38} + A_{171}^{16} A_{127}^8 A_{125}^{18} + A_{171}^{16} A_{125}^2 A_{127}^{16}$$
$$+ A_{171}^{16} A_{127}^4 A_{125}^{26} + A_{171}^{16} A_{125}^{34} + A_{175}^4 A_{125}^{30}$$
$$+ A_{171}^{64} A_{125}^2 A_{127}^8 + A_{171}^{64} A_{127}^4 A_{125}^{10} + A_{171}^{64} A_{125}^{18} = 0$$

$$\Rightarrow A_{187} := A_{125}^{142} + A_{125}^{385} A_{171}^2 + A_{125}^{383} A_{171}^8 + A_{171} A_{127}^2 A_{125}^4$$
$$+ A_{171} A_{127}^4 + A_{125}^3 A_{171}^4 A_{127}^2 + A_{125}^{510} A_{175}^4$$
$$+ A_{183} A_{125}^2 + A_{171} A_{125}^8$$
$$+ A_{175} A_{125}^6 + A_{125}^{510} A_{171}^4 A_{127}^4$$
$$+ A_{125}^5 A_{171}^4 A_{127} + A_{171}^4 A_{125}^7 + A_{125}^{510} A_{171}^{16} A_{127}^2$$
$$+ A_{125} A_{171}^{16} A_{127} + A_{171}^{16} A_{125}^3$$

$$I_{388}: A_{171}^8 A_{127}^{10} + A_{125}^{258} A_{127}^{16} + A_{175}^4 A_{125}^{257} + A_{125}^{274} A_{127}^8$$
$$+ A_{125}^{282} A_{127}^4 + A_{171}^4 A_{125}^{257} A_{127}^4 + A_{175}^2 A_{127}^4 A_{125}^{10}$$
$$+ A_{171}^8 A_{127}^6 A_{125}^8 + A_{171}^{32} A_{127}^6 + A_{175}^2 A_{125}^2 A_{127}^8$$
$$+ A_{175}^8 A_{127}^2 + A_{183}^2 A_{125}^2 A_{127}^4 + A_{191}^2 A_{125}^2$$
$$+ A_{125}^4 A_{171}^{32} A_{127}^4 + A_{125}^{12} A_{171}^8 A_{127}^4 + A_{125}^{14} A_{171}^2 A_{127}^4 = 0$$

$$\Rightarrow A_{191} := A_{125}^{510} A_{171}^4 A_{127}^5 + A_{125}^{128} A_{127}^8 + A_{125}^{383} A_{175}^2 + A_{125}^{136} A_{127}^4$$
$$+ A_{125}^{140} A_{127}^2 + A_{125}^{383} A_{171}^2 A_{127}^2 + A_{175} A_{127}^2 A_{125}^4$$
$$+ A_{125}^3 A_{171}^4 A_{127}^3 + A_{125}^{510} A_{171}^{16} A_{127}^3 + A_{175} A_{127}^4$$
$$+ A_{125}^{510} A_{175}^4 A_{127} + A_{183} A_{127}^2 + A_{171}^{16} A_{125} A_{127}^2$$
$$+ A_{171}^4 A_{127}^2 A_{125}^5 + A_{125}^6 A_{171} A_{127}^2$$

$$I_{392}: A_{125}^2 + A_{171}^6 = 0 \Rightarrow A_{171} := A_{125}^{341}$$

$$I_{404}: A_{127}^2 + A_{125}^{340} A_{175}^2 = 0 \Rightarrow A_{175} := A_{127} A_{125}^{341}$$

$$I_{412} := A_{125}^{97} + 1 = 0 \Rightarrow A_{125} := 1$$

$$I_{420}: A_{127}^2 + A_{183}^2 + A_{183}^4 = 0 \Rightarrow A_{127} := A_{183} + A_{183}^2$$

$$I_{428}: 1 = 0. \qquad \square$$

ACKNOWLEDGMENT

REFERENCES

[1] E. F. Assmus and J. D. Key, "Affine and projective planes," *Discrete Math.*, vol. 83, pp. 161–187, 1990.

[2] P. Charpin, "Codes cycliques étendus affines-invariants et antichaînes d'un ensemble partiellement ordonné," *Discrete Math.*, vol. 80, pp. 229–247, 1990.

[3] G. Cohen, "Distance Minimale et Enumération des Poids des Codes Linéaires," Thèse de 3ᵉ Cycle, ENST, Apr. 1976.

[4] ——, "On the minimum distance of some BCH codes," *IEEE Trans. Inform. Theory*, vol. 26, p. 363, May 1980.

[5] J.-L. Dornstetter, "Quelques resultats sur les codes BCH binaires en longueur 255," ENST stage rep., Annex, July 1982.

[6] H. J. Helgert and R. D. Stinaff, "Shortened BCH codes," *IEEE Trans. Inform. Theory*, vol. 19, pp. 818–820, Nov. 1973.

[7] T. Kasami and S. Lin, "Some results on the minimum weight of primitive BCH codes," *IEEE Trans. Inform. Theory*, vol. 18, pp. 824–825, Nov. 1972.

[8] T. Kasami, S. Lin, and W. W. Peterson, "Some results on cyclic codes which are invariant under the affine group and their applications," *Inform. Contr.*, vol. 11, pp. 475–496, 1967.

[9] ——, "New generalisations of the Reed–Muller codes—Part I: Primitive codes," *IEEE Trans. Inform. Theory*, vol. 14, pp. 189–199, Mar. 1968.

[10] T. Kasami and N. Tokura, "Some remarks on BCH bounds and minimum weights of binary primitive BCH codes," *IEEE Trans. Inform. Theory*, vol. 15, pp. 408–413, May 1969.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North-Holland, 1986.

[12] W. W. Peterson, *Error-Correcting Codes*. Cambridge, MA: MIT Press, 1961.

[13] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. 32, pp. 23–40, Jan. 1986.